VZCZCXRO0914
OO RUEHAST RUEHBI RUEHCI RUEHDBU RUEHLH RUEHNEH RUEHPW
DE RUEHNE #1052/01 1421226
ZNR UUUUU ZZH
O 221226Z MAY 09
FM AMEMBASSY NEW DELHI
TO RUEHC/SECSTATE WASHDC IMMEDIATE 6705
INFO RUCNCLS/ALL SOUTH AND CENTRAL ASIA COLLECTIVE
RUEHBJ/AMEMBASSY BEIJING 7694
RUEHLO/AMEMBASSY LONDON 6420
RUEHMO/AMEMBASSY MOSCOW 3434
RUEHKO/AMEMBASSY TOKYO 6351
RHMFIUU/DEPT OF HOMELAND SECURITY WASHINGTON DC
RHEFDIA/DIA WASHDC
RHMCSUU/FBI WASHINGTON DC
RUEHGV/USMISSION GENEVA 8337
RHEHAAA/WHITE HOUSE WASHDC
RUEAIIA/CIA WASHDC
RHEHNSC/NSC WASHDC
RUEIDN/DNI WASHINGTON DC
RUCNDT/USMISSION USUN NEW YORK 8071
RHMCSUU/HQ USCENTCOM MACDILL AFB FL
RHHMUNA/HQ USPACOM HONOLULU HI
RUEKJCS/JOINT STAFF WASHDC

UNCLAS SECTION 01 OF 08 NEW DELHI 001052

SENSITIVE
SIPDIS

FOR S/CT HILLARY BATJER JOHNSON AND S/CT PAUL SCHULTZ,
NCTC, DHS

E.O. 12958: N/A
TAGS: PGOV PREL PTER PK IN
SUBJECT: RESPONSE TO REQUEST FOR UPDATES ON INFORMATION ON
HOST GOVERNMENT PRACTICES-INFORMATION COLLECTION, SCREENING
AND SHARING

REF: STATE 032287

¶1. (SBU) The following information is provided in response to
reftel request for details of India,s immigration and border
controls.
¶A. (SBU) Immigration Data Bases and Traveler Information
Collection:
-- What computerized immigration databases are used to track
entries and exits? Foreigners Regional Registration Officers
(FRRO) uses a computerized entry/exit tracking system, but
these systems are not linked to a centralized database.
-- Is the computerized immigration database available at all
ports of entry (POE5)? Most air ports of entry and some land
ports of entry have access to such systems, but they are not
linked to a centralized database.
-- If immigration databases are available at some POEs, but
not all, how does the host government decide which POEs will
receive the tool? Apparently, this is determined by a
combination of factors to include: volume of crossings or
entries, affluence of the state containing the POE and the
perceived importance of the POE by the Ministry of Home
Affairs (MHA).
-- What problems, if any, limit the effectiveness of the
systems? The systems do not read biometric passports and are
isolated (not linked to a centralized database).
-- For example, limited training, power brownouts, budgetary
restraints, corruption, etc.? All of the above. Further
Police and other law enforcement and court agencies will
write requests to the Bureau of Immigration for input of
derogatory data, such as convictions, warrants etc. into the
lookout systems. This is a time delay. The state agencies do
not have electronic linking of such data to Bureau of
Immigration Computer Systems.
-- How often are national immigration databases updated? This
info has not been shared by MHA.
-- What are the country,s policies (legislation, mandates,
etc.) on collecting information from travelers arriving in
the country? India recently began requiring air carriers to
provide APIS info on travelers coming to India pursuant to an

amendment to the Foreigners Order, 1948 which was published in the Gazette of India on January 24, 2008.
-- Are there different policies for entry and exit at air, sea, and land POE5 and for domestic flights? It would appear as such, but MHA will neither confirm nor deny this. These different POEs are controlled by different entities such as the military, the Border Security Force (BSF), the Bureau of Indian Immigration and the state police. The Immigration services at the major International Airports in India and the Foreigners, registration work in five major cities, are handled by the Bureau of Immigration (BOI). The field officers in charge of immigration and registration activities at Delhi, Muxnbai, Kolkata, Chennai and Amritsar are called Foreigners Regional Registration Officers (FRRO5). Apart from the FRROs who look after the immigration/registration functions in the above mentioned five cities, the concerned Districts Superintendents of Police function as Foreigners Registration Officers (FROs) in all the states in the country.
-- What agency oversees the collection of traveler information? The Ministry of Home Affairs manages most of these activities in conjunction with the Indian Intelligence Bureau (IB), the Research and Analysis Wing (RAW) which is India,s foreign intelligence agency, the Central Industrial Security Forces (CISF), the Bureau of Civil Aviation Security (BCAS), the state police and the Bureau of Immigration (BOl).
-- What are the policies of the collecting agency to share that information with foreign governments? India shares information with foreign partners sparingly and only on a limited bi-lateral basis. The U.S. does not have an

Immigration Mutual Assistance Agreement with India at this time, so our requests for information are viewed on a case*by-case basis where responses are given sometimes or not at all. In March 2002 the Indian Parliament, in a rare joint session, passed the Prevention of Terrorism Act (POTA) over the objections of several opposition parties and in the face of considerable public criticism. The National Human Rights Commission, an independent government entity, criticized the measure finding the existing laws were sufficient to combat terrorism. The law codifies the Prevention of Terrorism Ordinance that in turn builds on the repealed Terrorists and Disruptive Activities (Prevention) Act (TADA). It gives law enforcement sweeping powers to arrest suspected terrorists, intercept communications, and curtail free expression. Critics argue that the experience of TADA and POTA shows that the power was often misused for political ends by authorities and that POTA does little to curb those excesses. POTA was repealed in the year 2004, as minority communities were targeted in India. After 26/11 the TADA was amended and the National Investigation Agency was established to collect and share information with foreign governments.
-- Does the host government collect Passenger Name Record (PNR) data on incoming commercial flights or vessels? Yes, but only as part of a pilot project mainly conducted at the international airports in Delhi and Mumbai.
-- Is this data used for intelligence or law enforcement purposes to screen travelers in a systematic way? Theoretically, yes. The GOl reports that this info will be shared with security, intelligence and border control agencies.
-- Does host government have any existing treaties to share PNR data? Not that we can determine. At this point in time, the Indian APIS data is not collected and stored in a format compatible with the European and American APIS systems.
-- If applicable, have advance passenger information systems (APIS), interactive advanced passenger information systems (IAPIS), or electronic travel authority systems been effective at detecting other national security threats, such as wanted criminals? Most likely, but no reports of this have been received from the GOl. It appears that APIS is used primarily to expedite immigration clearance at their woefully inadequate ports of entry.
¶B. (SBU) Watchlisting:

-- Is there a name-based watchlist system used to screen travelers at POEs? Yes.
-- What domestic sources of information populate the name-based watchlist, i.e. names of deported persons, terrorist lookouts, and criminal wants/warrants? lB terrorist lookouts and Interpol warrants mainly. However, all law enforcement agencies within India are able to enter lookouts, referred to as in India as Look Out Circulars (LOC) by forwarding a request to the Ministry of Home Affairs (MHA), Joint Director for Zimnigration. These requests follow a standard format, which includes at least three identifying factos such as full name, passport number, date and place of birth, and photo if available. The LOC indicators contact information for the originator of the LOC as well as the action requested by the originator if the subject of the lookout is encountered, to include detention. The LOC will remain in place for 12 months but can be extended.
-- If host government maintains a watchlst, how many records does the watchlist contain, and how many are terrorist-related? Unable to say; info not shared by GOl at this level.
-- Which ministry or office maintains the watchlist? Mainly the Indian Intelligence Bureau, who works closely with the Bureau of Immigration. Also, Bureau of Immigration, Foreign Regional Registration Office (FRRO), located at R.K. Puram,

New Delhi, is very uncooperative and reluctant to answer any questions concerning this information.
-- What international watchlists does the host government use for screening individuals, e.g. Interpol or TSA No Fly lists, UN, etc.? The Central Bureau of Investigation (CBI) Interpol disseminated all Interpol Red Notices to the border and along with Look Out Circulars (LOCs), Interpol lookouts are part of the watchlists. According to police sources, these watchlists are not combined and generally border officials will first check the LOCs watchlist, followed by Interpol notices.
-- What bilateral/multilateral watchlist agreements exist between host government and its neighbors? This info not shared at this level.
¶C. (SBU) Biometrics:
-- Are biometric systems in place at ports of entry (air, land, sea)? If no, does host government have plans to install such a system? Only at select airports as part of a pilot project involving e-passports for select Indian diplomats and government officials. India has recently initiated first phase deployment of Biometric e-Passport for Diplomatic Passport holders in India and abroad. The new passports have been designed indigenously by the Central Passport Organization, the India Security Press and lIT Kanpur. The passport contains a security chip with personal data and digital images. Initially, the new passports will have a 64KB chip with a photograph of passport holder and subsequently include the holder,s fingerprint(s). The biometric passport has been tested with passport readers abroad and is noted to have a 4 second response time which is less than that of a US Passport (10 second response time). The passport need not be carried in a metal jacket for security reasons as it first needs to be passed through a reader, after which generates access keys to unlock the chip data for reader access.
-- If biometric systems are available at some POES, but not all, how does the host government decide what POE5 will receive the tool? Delhi and Mumbai were chosen as most government officials fly via these POE5.
-- What biometric technologies, if any, does the host government use, i.e. fingerprint identification, facial recognition, iris recognition, hand geometry, retinal identification, DNA*based identification, keystroke dynamics, gait analysis? Fingerprint identification, digital photo and personal info.
-- Are the systems ICAO compliant? The Indian press reports indicate that the e-passport is ICAO compliant.
-- Are biometric systems integrated for all active POE5? No.
-- What are the systems and models used? Infineon Technologies (FSE/NYSE: IFX) was announced as the supplier of the contactless security microcontrollers for India,s

electronic passport program. The India electronic passport project utilizes the SLE 66CLX800PE security microcontroller from Infineon which provides advanced performance and high execution speeds and was specifically designed for use in electronic passports, identity cards, e-government cards and payment cards. The security microcontroller features a crypto-coprocessor and can operate at very high transaction speeds of up to 848 kbits per second even if elevated encryption and decryption operations have to be calculated. In addition, the SLE 66CLX800PE offers all contactiess proximity interfaces on a single chip: the ISO/IEC 14443 Type B interface and Type A interface which are both used for communication between electronic passports and the respective readers, and the ISO/IEC 18092 passive mode interface which is used in transport and banking applications mainly in Japan. Infineon is currently the world,s only chip card IC provider offering contactless microcontrollers with all relevant contactless proximity interfaces on a single chip. The SLE 66CLx800PE is also compliant with global ICAO (International Civil Aviation Organization) standards for

electronic passports. (source: WEBWIRE * Tuesday, March 03, 2009)
-- Are all passengers screened for the biometric or does the host government target a specific population for collection (i.e. host country nationals)? At present, they only screen their diplomats or government officials that have been issued Indian e-passports.
-- Do the biometric collection systems look for a one to one comparison (ensure the biometric presented matches the one stored on the e-Passport) or one too many comparisons (checking the biometric presented against a database of known biometrics)? Not sure.
-- If biometric systems are in place, does the host government know of any countermeasures that have been used or attempted to defeat biometric checkpoints? That info has not been shared.
-- What are the host government,s policies on collecting the fingerprints of travelers coming into the country? India does not collect fingerprints at this point in time.
-- Which agency is responsible for the host government,s fingerprint system? The Indian Government rarely collects fingerprints. When collected, it is done by local police in local jails, but only with the consent of the prisoner.
-- Are the fingerprint programs in place NIST, INT-I, EFTS, UK1 or RTID compliant? No.
-- Are the fingerprints collected as flats or rolled? We are not sure of the exact procedure the GOl uses to collect fingerprints, it should be noted that the India Bureau of Immigration and FRRO do not collect fingerprints.
-- Which agency collects the fingerprints? State and city police.
¶D. (SBU) Border Control and Screening:
-- Does the host government employ software to screen travelers of security interest? Yes, but these systems are not yet networked or linked to a central database.
-- Are all travelers tracked electronically, or only non-host- country nationals? Only those with machine-readable passports, but the systems are not linked to a centralized database. Only host-country officials who have been issued e-passports are tracked as far as we can tell.
-- What is the frequency of travelers being &waived through8 because they hold up what appears to be an appropriate document, but whose information is not actually recorded electronically? Frequently with GOl employees or officials.
-- What is the estimated percentage of non-recorded crossings, entries and exits? Though we are unable to affix a set percentage we can state that non-recorded crossings are suspected to be very high at land border crossings due to corruption, apathy and selfpreservation.
-- Do host government border control officials have the authority to use other criminal data when making decisions on who can enter the country? The Border Security Force (BSF) which guards the India-Pakistan and the India-Bangladesh

borders, the Indo-Tibetan Border Police Force (ITBPF) which is deployed along the India- Tibet (China) border and the Assam Rifles (AR) which is deployed along the India-Myanmar border, are usually the first representatives of the Indian system which travelers may encounter when they enter or exit India by land routes.
The vastness of the border terrain make it difficult to physically man the entire international borders of India. The gaps in the border left unguarded, are often used by criminals to illegally enter/exit the Indian territory. If caught while entering illegally, the authorities may return the interloper across the border. The border guarding force may interrogate and detain the person as permissible under the law of the land, at the border itself, pending decision by the administrative authorities. In all such cases, the

person will have to be ultimately handed over to the local police who will exercise their powers under relevant provisions of the Criminal Procedure Code (Cr.PC).
It is part of the duty and responsibility of the border authorities to rule out any criminal or anti-national intent on the part of the traveler who may be entering the country for mala fide purposes. If caught illegally exiting India, the person may be handed over to the local police for investigation and for further action according to law. In cases where the traveler is found in possession of invalid travel documents or in cases of violation of any other Indian law, the traveler may be detained by the border authorities at the border post itself and are then handed over to the local police for investigation. In all such instances, after the registration of a case on the basis of a First Information Report, the police would lodge the accused mala fide traveler in the area prison and produce him/her in the local court for trial in conformity with the provisions of CrPC.
-- If so, please describe this authority (legislation, mandates, etc). Indian Penal Code, the Foreigners Act, 1946, Foreigners Order, the Passport Act 1967 and the Criminal Procedure Code of India, 1973 (Cr.PC).
-- What are the host government,s policies on questioning, detaining and denying entry to individuals presenting themselves at a point of entry into the country? The engagement of the BSF and their power to arrest, detain and question civilians in non- war situations is governed by the Criminal Procedure Code of India, 1973 (Cr.PC). This law that regulates the operation of law enforcement officers, including paramilitary units like the BSF in a civilian settings.
-- Which agency would question, detain, or deny entry? Depending on the type of POE, the region, sensitivity, etc, usually the Indian Military Intelligence, the Border Security Force, the State Police, the Bureau of Immigration or the Intelligence Bureau would question detain or deny entry.
-- How well does information sharing function within the host government, i.e., if there is a determination that someone with a valid host-government visa is later identified with terrorism, how is this communicated and resolved internally? Not sure how this is exactly done. As mentioned earlier the United States does not have an Immigration Mutual Assistance Agreement (IMAA) at this time. CBP has discovered the Bureau Of Immigration and FRRO to be uncooperative and non sharing, except in their time of need when they will call the residence for information concerning passengers at the Airports.
¶E. (SBU) Passports:
-- Does the host government issue a machine-readable passport containing biometric information? No.
-- If so, what biometric information is included on the document, i.e. fingerprint, iris, facial recognition, etc.? N/A
-- If not, does host government plan to issue a biometric document in the future? When? Yes, facial recognition is planned starting (estimate) January 2010. A second phase might include fingerprints.
-- If the host government issues a machine-readable passport

containing biometric information, does the host government share the public key required to read the biometric information with any other governments? N/A
-- If so, which governments? N/A
-- Does the host government issue replacement passports for full or limited validity (i.e. the time remaining on the original passports, fixed validity for a replacement, etc.)? Full validity is generally issued. A one-year passport may be issued if expedited service is requested.
-- Does the host government have special

regulations/procedures for dealing with &habitual8 losers of passports or bearers who have reported their passports stolen multiple times? Yes, according to contacts, but the details of the procedures were not publically available. As per the FRRO the Bureau of Immigration and FRRO, lookouts are placed on those habitual losers of passports or bearers who have reported their passports stolen multiple times. The subject is then detained and questioned when encountered in their entry/exit registration lookout systems.
-- Are replacement passports of the same or different appearance and page length as regular passports (do they have something along the lines of our emergency partial duration passports)? Same appearance.
-- Do emergency replacement passports contain the same or fewer biometric fields as regular-issue passports? Same appearance.
-- Where applicable, has Post noticed any increase in the number of replacement or &clean8 (i.e. no evidence of prior travel) passports used to apply for U.S. visas? No.
-- Are replacement passports assigned a characteristic number series or otherwise identified? No.
¶F. (SBTJ) Fraud Detection:
-- How robust is fraud detection and how actively are instances of fraud involving documents followed up? Local immigration and police have been very responsive to requests and complaints filed by USG personnel, particularly part of the ARSO/I program, targeting fraudulent documents. During FY 2008, local police arrested 280 persons countrywide for various violations of the Indian Penal Code (IPC) related to document fraud. In all cases, local police require a written complaint, called a First Incident Report (FIR), to be filed before taking action. Neither immigration nor police officials will routinely take action against a traveler until the traveler presents the fraudulent documents at the immigration check point.
Likewise, Airline Liaison Officers (ALOs) and document advisors from the UK, Canada, Austria, and Germany working at the airports in New Delhi and Mumbai have reported that immigration and police will take document fraud cases referred by these officers. Immigration officials at the primary international airports do have examination equipment such as U/V lamps and training on basic document detection. However, fraud detection varies widely depending on the volume of crossings or entries, affluence of the state containing the POE and the resources and personnel assigned to the POE by the Ministry of Home Affairs (MHA). Immigration officials tend to detect more fraud with foreign documents as these travelers often receive more scrutiny that travelers with Indian documents.
-- How are potentially fraudulently issued documents taken out of circulation, or made harder to use? In cases where immigration officials have referred the case to police and the individual has been arrested, the documents are normally seized as part of the criminal case. However, it is normal for the immigration officials to refuse entry and return the traveler to the originating country with the same fraudulent documents. GoI officials do not routinely cancel, mark, or seize these documents, particularly for transit passengers. It is not uncommon for Airline Liaison Officers from the U.K. Canada, Germany, or Austria, to encounter or off-load the same traveler presenting the same fraudulent document on multiple occasions. GoI officials do not routinely issue a substitute transportation letter for the deported traveler and seize the fraudulent, counterfeit, or altered document.

¶G. (SBU) Privacy and Data Security:
-- What are the country,s policies on records related to the questioning, detention or removal of individuals encountered at points of entry into the country? These records would fall under Under the Right to Information (RTI) Act of 2005 as

well as any other internal policy and procedure documents.
-- How are those records stored, and for how long? Unknown.
-- What are the country,s restrictions on the collection or use of sensitive data? Unknown.
-- What are the requirements to provide notice to the public on the implementation of new databases of records? Unknown.
-- Are there any laws relating to security features for government computer systems that hold personally identifying information? Unknown.
-- What are the rules on an individual,s ability to access data that homeland security agencies hold about them?
Under the Right to Information (RTI) Act of 2005, Indian citizens as well as overseas Indian citizens (OCI,s) and Persons of Indian Origin (PIOs), can request access to information held about them within Indian files. Under the Act, information is defined as any material in any form, including records, documents, memos, e* mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law for the time being in force. Likewise, the Act includes records in the forms of documents, manuscripts, files, microfiche, and copies of documents. Requesters may ask for certified copies of the documents as well as the information in the form of a diskette, video tapes, or any electronic medium in which it is stored.
The Act does allow the G0I to withhold release of information in cases which affect issues of sovereignty, law enforcement, security, or bi-lateral foreign relations. The Act specifically allows the Gol to reject from disclosure, "information received in confidence from foreign Government" (section 8(1) (f) and "information, the disclosure of which would endanger the life or physical safety of any person or identify the source of information or assistance given in confidence for law enforcement or security purposes" (section 8(l)(g)). To enhance the security of any information provided to the Gol, it is recommended that a provision be included by the USG that the information being provided to the Gol be exempted from disclosure under the RTI Act of 2005, sections 8(1) (f) and/or 8(1) (g)
Requesters under the RTI Act are required to state that they will not circulate, use, or share information with any person or in any manner which would be detrimental to the Unity and Sovereignty or against the Interest of India. However, it is unknown how vigorously this provision is enforced.
-- Are there different rules for raw data (name, date of birth, etc.) versus case files (for example, records about enforcement actions)? Unknown.
-- Does a non-citizen/resident have the right to sue the government to obtain these types of data? Under the RTI Act, only citizens, OCI,s (Overseas Citizens of India) and PlO,s (Persons of Indian Origin) can ask for information.
Non-Indian citizens who are married to an Indian citizen do qualify for PlO status and would therefore be entitled to request information under the RTI Act. Indian citizens overseas can file a request with the closest Indian Embassy or Consulate. The Act extends to all of India except the State of Jammu and Kashmir.
¶H. (SBU) Identifying Appropriate Partners:
Department would appreciate post,s in-house assessment of whether host government would be an appropriate partner in data sharing. Considerations include whether host government watchlists may include political dissidents (as opposed or in addition to terrorists), and whether host governments would share or use U.S. watchlist data inappropriately, etc.
-- We have no information to answers these questions.
-- Are there political realities which would preclude a country from entering into a formal data-sharing agreement

with the U.S.?
-- Is the host country's legal system sufficiently developed to adequately provide safeguards for the protection and nondisclosure of information?
-- How much information sharing does the host country do internally? Is there a single consolidated database, for example? If not, do different ministries share information amongst themselves?
-- How does the country define terrorism? Are there legal statutes that do so?
BURLEIGH